Základy algebry

Milan Radojčić

SSPŠaG – KBB

7. listopadu 2025

Hlavní body

Grupa

Modulární aritmetika

Rozšířený Euklidův algoritmus

Vektorové prostory

Hlavní body

Grupa

Modulární aritmetika

Rozšířený Euklidův algoritmus

Vektorové prostory

Definice

Mějme množinu M a binární operaci $\bullet$. Pokud platí:

1. **uzavřenost**: $(\forall a, b \in M)((a \bullet b) \in M)$,
2. **asociativita**: $(\forall a, b, c \in M)((a \bullet b) \bullet c = a \bullet (b \bullet c))$,
3. **existence neutrálního prvku**: $(\exists e \in M)(\forall a \in M)(a \bullet e = e \bullet a = a)$,
4. **existence inverzního prvku**: $(\forall a \in M)(\exists i \in M)(a \bullet i = i \bullet a = e)$,[1]

tak dvojici $(M, \bullet)$ nazýváme **grupou**.

Pomněnka

Tuto definici se naučte, budu ji po Vás chtít u testu.

[1] Inverzní prvek pro a značíme a^{-1}.

Příklady grup

Je $(\mathbb{Z}, +)$ grupa? Ano, všechny podmínky jsou splněny.

Je $(\mathbb{N}, +)$ grupa? Není, neexistují inverze.

Je $(\mathbb{Q} \setminus \{0\}, \cdot)$ grupa? Ano.

Je $(\mathbb{Z} \setminus \{0\}, \cdot)$ grupa? Ne, také chybí inverze.

Je množina lichých čísel a sčítání grupa? Není, nejsou uzavřené. Např. $1 + 1 = 2$.

Abelovská grupa

Definice

Mějme grupu $(M, \bullet)$ a $a, b \in M$. Platí-li navíc: $(\forall a, b \in M)(a \bullet b = b \bullet a)$ tak se jedná o **abelovskou grupu**.

Poznámka

Této vlastnosti se také říka **komutativita**.

Všechny příklady grup na minulém slidu byly také *abelovské*.

Poznámky

- Přirozeně se nabízí *zrušení* některých požadavků na grupu.
  - Například bez *existence inverzních prvků* dostaneme strukturu, které se říká *monoid*.

Hlavní body

Modulární aritmetika

Definice

Pro $m, n \in \mathbb{Z}$ a $n \geq 2$: $m \mod n$ označíme zbytek po celočíselném dělení m číslem n.

Ukázka modulování *"za běhu"*

$$9 +_7 6 +_7 6 = 2 +_7 6 +_7 6 = 8 +_7 6 = 1 +_7 6 = 7 \mod 7 = 0$$

Pro jednoduchost zápisu definujme tuto množinu a operace:

Definice

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$$
$$a +_n b = (a + b) \mod n$$
$$a \cdot_n b = (a \cdot b) \mod n$$

Je $(\mathbb{Z}_n, +_n)$ grupa pro libovolné n? Projděme si všechny vlastnosti a ověřme, že platí.

1. **Uzavřenost** – Platí z definice $+_n$. Po provedení operace m mod n nemůžeme získat číslo větší než $n - 1$, tím pádem zůstáváme v množině $\mathbb{Z}_n$.
2. **Asociativita** – Sčítání (i modulo n) je asociativní, tato vlastnost tedy platí.
3. **Existence neutrálního prvku** – Tato vlastnost je opět triviální, pro sčítání je neutrální prvek 0, tedy platí $0 +_n a = a +_n 0 = a$ pro libovolné $a \in \mathbb{Z}_n$.
4. **Existence inverzního prvku** – Pro každé $a \in \mathbb{Z}_n$ existuje inverzní prvek $-a$, který vypadá takto: $-a = n - a$.

Věta

$(\mathbb{Z}_n, +_n)$ je grupa pro libovolné n. Tuto grupu budeme značit $\mathbb{Z}_n^+$.

Pomněnka

Toto si také zapamatujte, hlavně značení.

Přesvědčili jsme se, že $(\mathbb{Z}_n, +_n)$ je grupou bez ohledu na volbu n. Jak je to ale s $(\mathbb{Z}_n, \cdot_n)$, je to grupa?

- První tři body jsou stejné.
- Jak je to s inverzemi?
  - Inverzi pro 0 nikdy nenajdeme, ale můžeme se omezit na $\mathbb{Z}_n \setminus \{0\}$,
  - Ale co ostatní? Zkusme si ukázat na příkladu!

Nalezení inverze $2^{-1} \mod 5$

$2 \cdot 1 = 2, 2 \cdot 2 = 4, 2 \cdot 3 = 6 = 1$

$2^{-1} \mod 5 = 3!$

Nalezení inverze $2^{-1} \mod 4$

$2 \cdot 1 = 2, 2 \cdot 2 = 0, 2 \cdot 3 = 2$

Zjistili jsme tedy, že $(\mathbb{Z}_4 \setminus \{0\}, \cdot_4)$ není grupa a je to tím, že 4 a 2 jsou čísla soudělná.

Máme tedy otázku: „Jak vybrat n, aby všechna čísla menší než n byla s ním nesoudělná?“

Věta

Je-li n prvočíslo, poté $(\mathbb{Z}_n \setminus \{0\}, \cdot_n)$ je grupa. Tuto grupu budeme značit $\mathbb{Z}_n^*$.

Pomněnka

Zapamatovat (zase hlavně značení.)

Těleso

Přirozeně bychom chtěli dát nějakou množinu a dvě operace dohromady do nějakého objektu.

Definice

Mějme množinu M, a binární operace $+$ a $\cdot$, pokud platí, že

1. $(M, +)$ je Abelovská grupa,
2. pokud 0 je neutrální prvek vůči sčítání, tak $(M \setminus \{0\}, \cdot)$ je grupa,
3. distributivní zákony zleva a zprava,

$$a, b, c \in M, \quad a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{a} \quad (b + c) \cdot a = b \cdot a + c \cdot a$$

tak trojici (M, +, ·) nazýváme **tělesem**.

Pomněnka

Tuto definici se naučte, budu ji po Vás chtít u testu.

Těleso

Věta

Množina $\mathbb{Z}_p$ a operace $+_p$ a $\cdot_p$ tvoří těleso, když p je prvočíslo. Toto těleso budeme značit $\mathbb{Z}_p$.

Pomněnka

Také si zapamatujte, hlavně značení.

Různé poznámky

- Stejně jako jsme mohli zrušit některé požadavky u grup, tak je můžeme zrušit i u tělesa.
  - Pokud nám například stačí, že $(M, \cdot)$ je *monoid* místo grupy, tak získáme *okruh*.
- Zájemcům o více informací o abstraktní algebře dopručuji tento playlist videí.

Hlavní body

Problém nalezení inverze

Zatím umíme nalézt inverzi jenom tím, že zkusíme všechny prvky z grupy. Tento přístup není vůbec efektivní a naštěstí známe lepší způsob.

Definice

Číslo $c \in \mathbb{N}$ je **největším společných dělitelem** čísel $a, b \in \mathbb{Z}$, značíme $c = \gcd(a, b)$, pokud je jejich společný dělitel a zároveň je celočíselným násobkém každého jiného jejich společného dělitele.

Rozšířený Euklidův algoritmus

Věta

Mějme $a, b \in \mathbb{Z}$. Pak platí:

$$(\exists k, l \in \mathbb{Z})(\gcd(a, b) = k \cdot a + l \cdot b).$$

Tento vztah se nazývá **Bézoutova rovnost**.

Rozšířený Euklidův algoritmus nám říká jak najít $\gcd(a, b)$, l a k.
Ale jak nám toto pomůže? Tomu se na hodině věnovat pro jednoduchost nebudeme. Ve skriptech je celé vysvětlení.

Ukázka REA

r	α	β	q
$a = 277$	1	0	
$b = 194$	0	1	1
83	1	-1	2
28	-2	3	2
27	5	-7	1
1	-7	**10**	

Kontrola: $194 \cdot 10 \mod 277 = 1940 \mod 277 = 1$

Bonusový úkol

- Jako bonusový úkol můžete naimplementovat REA.
  - Klidně v nějakém jiném jazyce než C#, ale nejprve se domluvte se mnou, že to je ok.
- Pseudokód algoritmu je ve skriptech.

Hlavní body

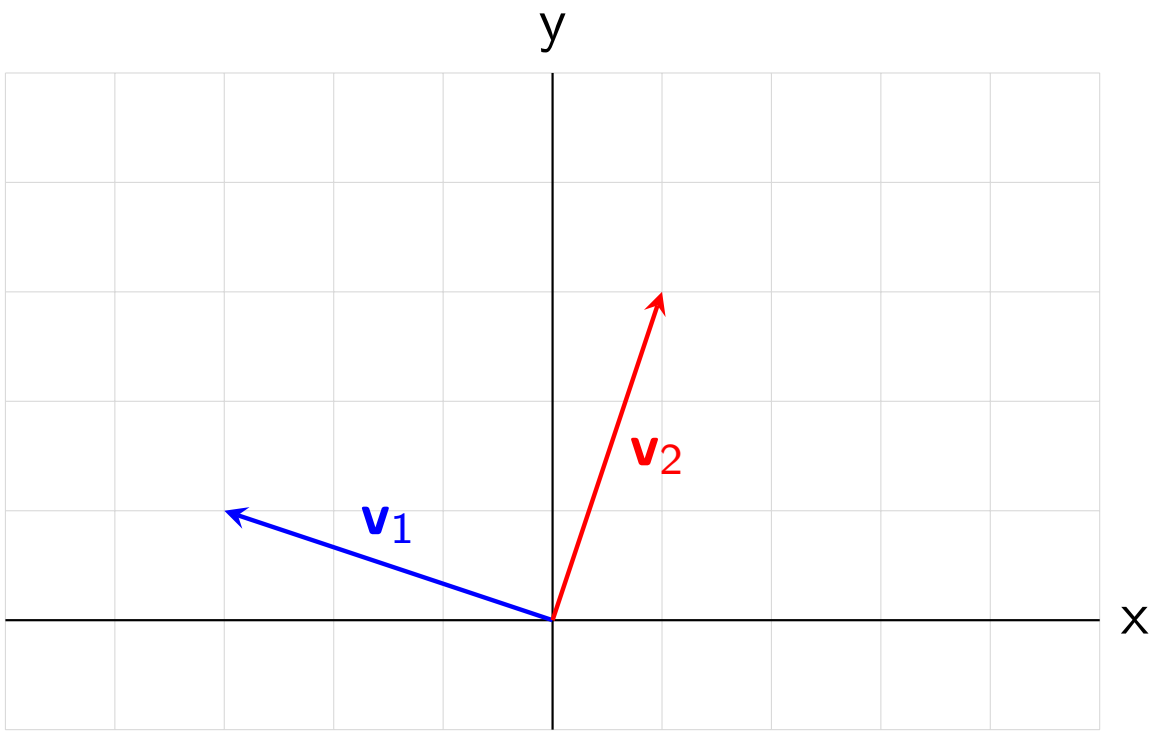
Grupa

Modulární aritmetika

Rozšířený Euklidův algoritmus

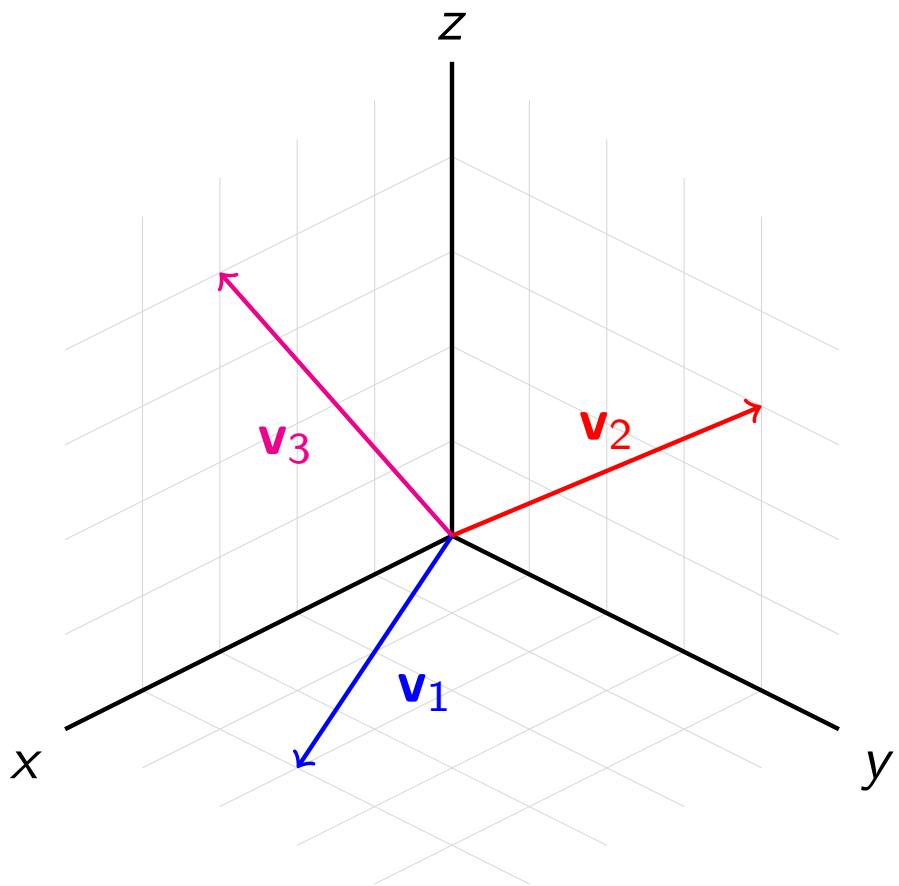
Vektorové prostory

Co je to vektorový prostor?



$$\mathbf{v}_1 = \begin{pmatrix} -3 \\ 1 \end{pmatrix} \quad \mathbf{v}_2 = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$$

Co je to vektorový prostor?



Sčítání vektorů

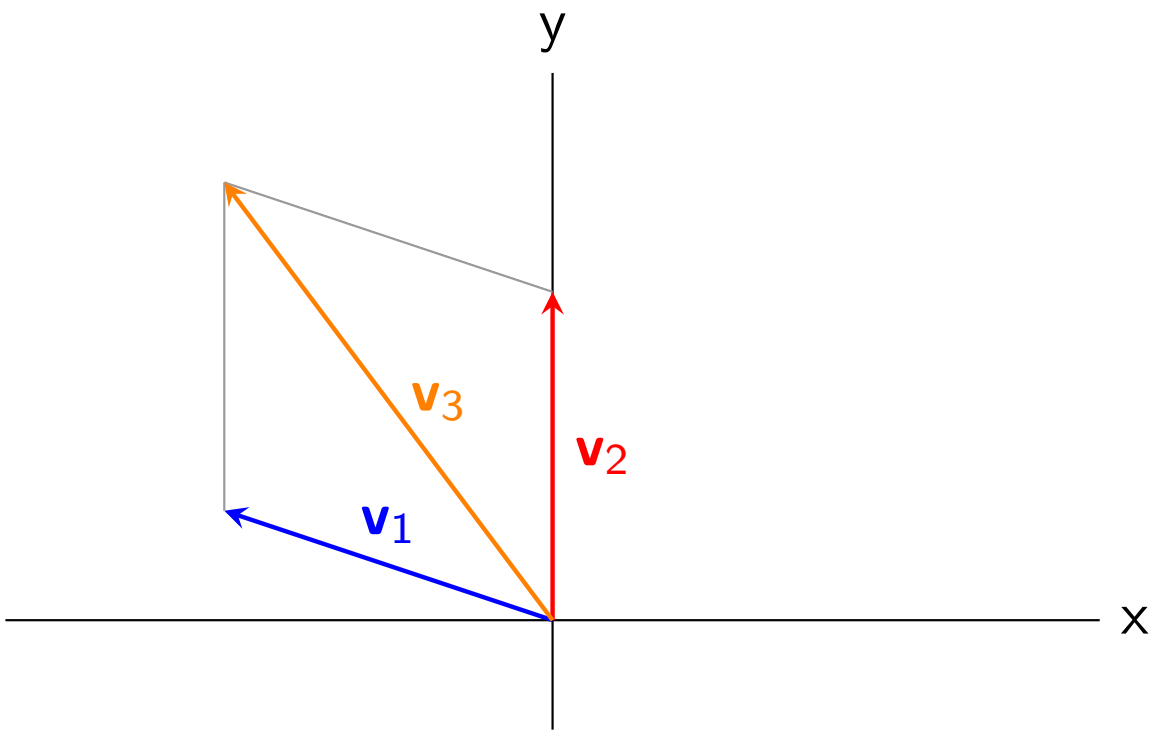
Vektory sčítáme po složkách:

$$\begin{pmatrix} 1 \\ 2 \end{pmatrix} + \begin{pmatrix} 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 4 \\ 6 \end{pmatrix}$$

Obecně:

$$\begin{pmatrix} a_1 \\ a_2 \\ \dots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ \dots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 \\ \dots \\ a_n + b_n \end{pmatrix}$$

Sčítání vektorů



$$\mathbf{v}_1 = \begin{pmatrix} -3 \\ 1 \end{pmatrix} \quad \mathbf{v}_2 = \begin{pmatrix} 0 \\ 3 \end{pmatrix} \quad \mathbf{v}_3 = \mathbf{v}_2 + \mathbf{v}_1$$

Škálování vektorů

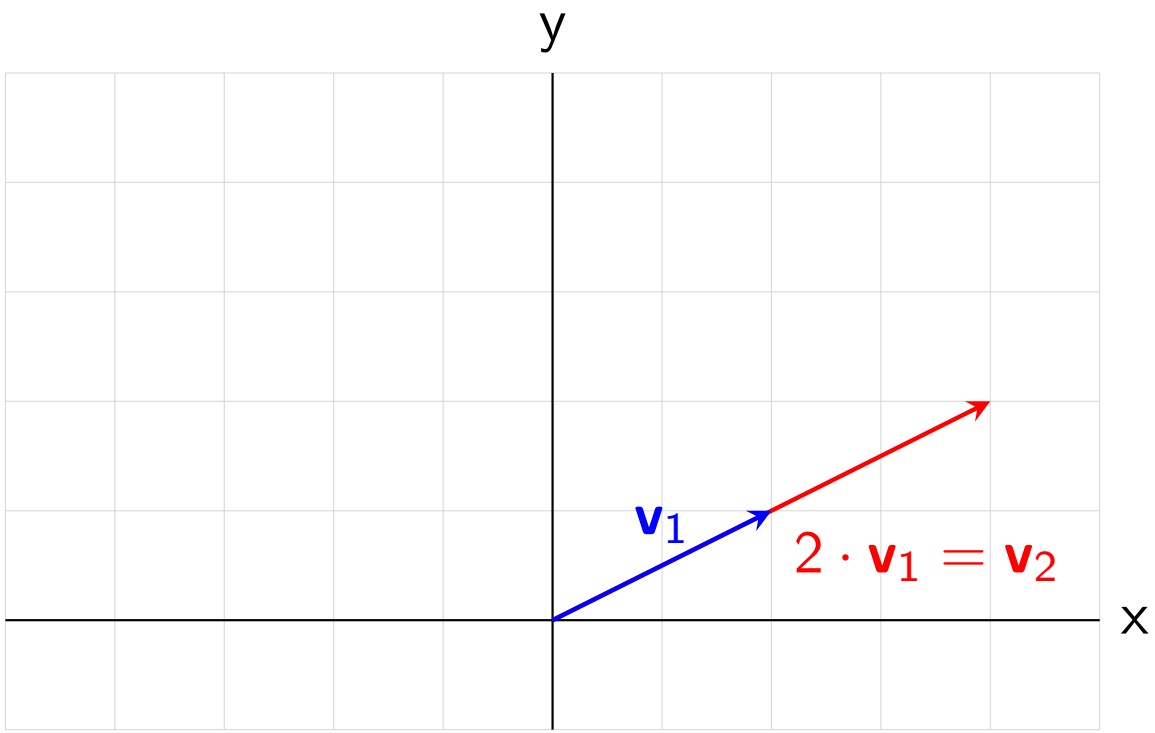
Vektory škálujeme tak, že všechny složky vynásobíme skalárem:

$$3 \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 3 \\ 6 \end{pmatrix}$$

Obecně:

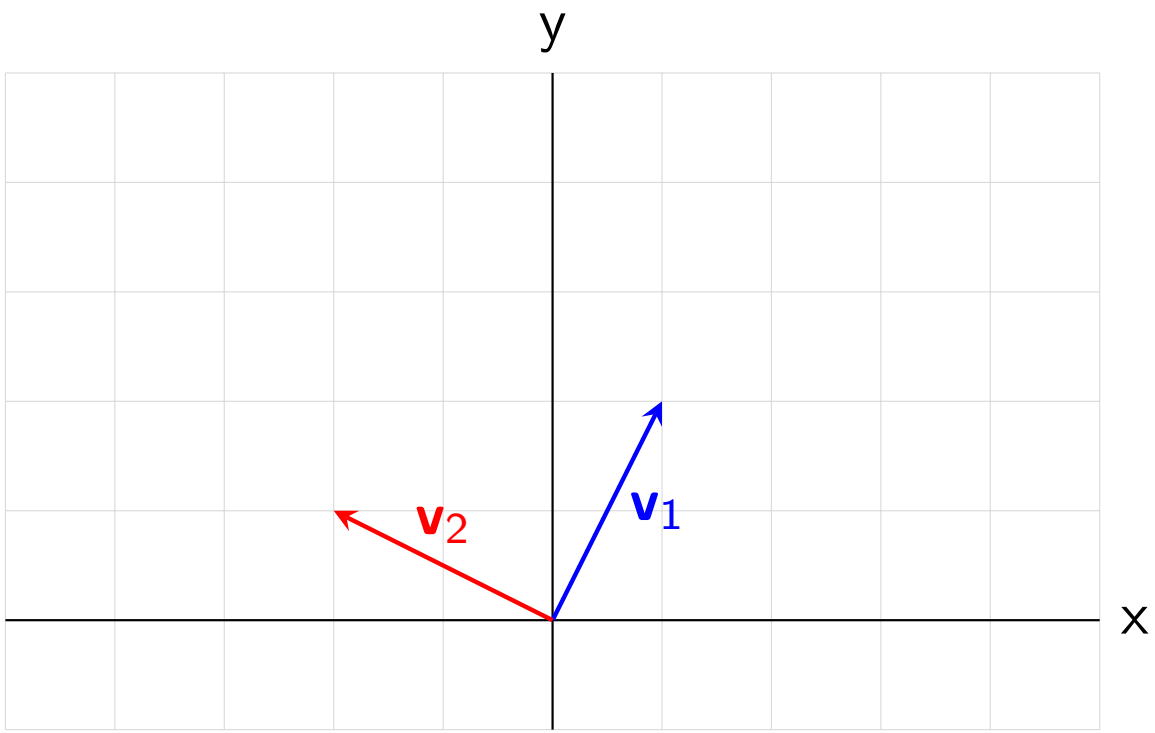
$$\alpha \cdot \begin{pmatrix} a_0 \\ a_1 \\ \dots \\ a_n \end{pmatrix} = \begin{pmatrix} \alpha \cdot a_0 \\ \alpha \cdot a_1 \\ \dots \\ \alpha \cdot a_n \end{pmatrix}$$

Škálování vektorů



$$\mathbf{v}_1 = \begin{pmatrix} 2 \\ 1 \end{pmatrix} \quad \mathbf{v}_2 = 2 \cdot \mathbf{v}_1 = \begin{pmatrix} 4 \\ 2 \end{pmatrix}$$

Násobení vektoru maticí



$$\mathbf{A} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \mathbf{v}_1 = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \quad \mathbf{v}_2 = \mathbf{A} \cdot \mathbf{v}_1$$

Násobení vektoru maticí

Pro matici 2×2:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = b_1 \cdot \begin{pmatrix} a_{11} \\ a_{21} \end{pmatrix} + b_2 \cdot \begin{pmatrix} a_{12} \\ a_{22} \end{pmatrix}$$

Obecně (matice $n \times m$):

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{pmatrix} \cdot \begin{pmatrix} b_1 \\ b_2 \\ \cdots \\ b_m \end{pmatrix} =$$

$$b_1 \cdot \begin{pmatrix} a_{11} \\ \cdots \\ a_{n1} \end{pmatrix} + b_2 \cdot \begin{pmatrix} a_{12} \\ \cdots \\ a_{n2} \end{pmatrix} + \cdots + b_m \cdot \begin{pmatrix} a_{1m} \\ \cdots \\ a_{nm} \end{pmatrix}$$

Poznámky

- Zajímavým speciálním příkladem matice je **jednotková matice**:

$$\mathbf{E}_n = \begin{pmatrix} \mathbf{1} & 0 & \cdots & 0 \\ 0 & \mathbf{1} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \mathbf{1} \end{pmatrix}$$

  - Je zajímavá, protože *nic nedělá* (nemění vektory).
- Dále máte ve skriptech příklady matic *rotace* a *reflekce*.
- Pro zájemce o lineární algebru lze doporučit sérii videí od 3Blue1Brown.